

2518(4)(b)). The statute therefore cannot be interpreted to provide that a Title III order is directed solely to the interception of a particular individual's conversations, whether that person is the target of a criminal investigation or the subscriber to a particular telephone line. On the contrary, the order authorizes the interception of communications that take place over specific telecommunications facilities and relate to a particular criminal offense -- the identity of individual speakers need be specified only "if known."

In light of this statutory scheme, the Supreme Court has specifically held that a Title III order authorizes law enforcement to intercept a conversation that takes place over facilities subject to an interception order even if none of the parties to the conversation is named in the order itself. United States v. Kahn, 415 U.S. 143 (1974).¹⁰ The Supreme Court in Kahn recognized that "when there is probable cause to believe that a particular telephone is being used to commit an offense but no particular person is identifiable, a wire interception order may, nonetheless, properly issue under the statute."¹¹ 415 U.S. at 157. The Court explained that interception orders frequently seek to identify

¹⁰ TIA suggests that Kahn implies that "Section 2518 only authorizes law enforcement access to communications that can be heard over the targeted facilities." TIA Comments at 37. This contention is obviously wrong, because the statute now expressly provides for the interception of "electronic communications," defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature." 18 U.S.C. § 2510(12) (added in 1986 as part of the Electronic Communications Privacy Act). Moreover, the statute defines "interception" as "the aural or other acquisition" of communications. 18 U.S.C. § 2510(4).

¹¹ AirTouch incorrectly cites the Supreme Court's decision in United States v. Donovan, 429 U.S. 413 (1977), for the proposition that Title III orders that fail to name individuals violate the Fourth Amendment's particularity requirement. AirTouch Comments at 11 n.36. But Donovan holds, in the very passage from the opinion that AirTouch quotes, that "a wiretap application must name an individual if the Government has probable cause to believe that the individual is engaged in criminal activity." Donovan, 429 U.S. at 428 (emphasis added). To the extent that the government has probable cause to believe that the facilities are being used to commit an offense, but

(continued...)

individuals who are involved in criminal activity but who are unknown to law enforcement. See *id.* at 156-157. Interception orders serve the same investigatory purpose today. See Joint Hearings at 18 (prepared statement of FBI Director Freeh) ("Electronic surveillance is critical in the monitoring of drug traffickers' 'communications networks,' providing law enforcement with the ability to identify all of the organization's drug traffickers and their illegal proceeds").

Many commenters seem to assume that the individual who sets up the conference call and whose facilities are under surveillance must invariably have some connection with criminal activity. See, e.g., CDT Comments at 38 (stating that the FBI's concern is to "listen to the communications of a target"); SBC Comments at 8-9 (complaining that law enforcement seeks to intercept communications "regardless of whether or not the target party, *i.e.* the party named in the court order, is actually on the line"); EPIC Comments at 23 n.67 (claiming that "law enforcement with authority to monitor only the *subject's* conversation is not permitted to trace conversations on the facilities once the subscriber disconnects") (underlining added). But there is no basis for such an assumption -- on the contrary, Title III expressly contemplates that telecommunications facilities are subject to surveillance when they "are being used, or are about to be used, in connection with the commission of" a criminal offense, without regard to the identity or possible culpability of the subscriber. Indeed, an innocent subscriber might well set up a conference call for two targets of a criminal investigation, both named in an order that authorized interception of communications carried on the subscriber's facilities. Under the commenters' view of Title III, law enforcement

¹¹(...continued)

lacks probable cause with regard to a particular individual, there is no constitutional or statutory requirement that the individual be named.

would be authorized to monitor only those portions of the conference call in which the subscriber participated, and would be barred from intercepting any conversations that took place between the two suspected criminals while the subscriber was on hold, or had left the conversation permanently. Indeed, the same would be true for non-conference calls -- if a drug dealer's girlfriend called a confederate from her (tapped) telephone, gave the handset to her boyfriend and left the house, then, under the commenters' mistaken view of Title III, law enforcement would be unable to monitor the call. Title III, however, expressly authorizes interception under such circumstances.

There is therefore no legal basis for the commenters' claim that law enforcement lacks statutory authority to intercept the "held" portions of conference calls if a "subject" who was a party to an earlier portion of the conversation is no longer a participant. On the contrary, law enforcement's interception authority under Title III extends to all conversations that can be intercepted through the specified telecommunications facilities, regardless of the identity of the speakers. Much of the opposition on this point is thus based upon a misperception of Title III law.¹²

Unlike many other commenters, TIA properly acknowledges that Title III "allows interception of communications by persons other than intercept subject[s] who use the facilities of the intercept subject." TIA Comments at 34-35. However, TIA maintains that Title III nonetheless does not permit law enforcement to intercept the "held" portions of conference calls because to do so "would effect a huge expansion of the facilities doctrine." Ibid. According to TIA, the "facilities

¹² One commenter argues that access to the "held" portions of conference calls "is specifically denied by 103(a)(4) of CALEA." ATR Comments at 18. Section 103(a)(4), however, merely requires carriers to perform interceptions in a manner that protects "the privacy and security of communications * * * not authorized to be intercepted." Nothing in Section 103(a)(4) purports to narrow the scope of law enforcement's interception authority -- rather, the statute imposes requirements regarding communications that are not subject to interception under existing authority.

doctrine" is "limited by the requirement that the intercept involve the actual telephone or other physical facilities of the intercept subject -- as opposed to the entire system or network to which the telephones are attached." Ibid. TIA is factually mistaken in asserting that law enforcement seeks the capacity to intercept the calls carried over an "entire system or network"; moreover, its legal analysis is wrong as well.

The "facilities" at issue here are telecommunications facilities that carry "wire, oral or electronic communication[s]." 18 U.S.C. § 2518(1). As we have explained, the purpose of Title III is to authorize the interception of calls carried on specific telecommunications facilities if there is probable cause to believe that such calls will include "particular communications concerning [a specified criminal] offense." 18 U.S.C. § 2518(3)(a). Obviously, Title III cannot be read in a manner that causes changes in technology to render it obsolete. Restricting "facilities" under Title III to specific physical equipment such as the subscriber's local loop, or even the physical components of a carrier's switch, would greatly undermine the statute's effectiveness in the current telecommunications universe, and would frustrate Congress's purpose in giving interception authority to law enforcement. Instead, the term "facilities" must be understood functionally, just as it always has been, as the "communications pathway" where the communications are to be intercepted, regardless of where that pathway may physically be found. DOJ/FBI Petition at 28 n.10.¹³

¹³ TIA suggests that unless the term "facilities" refers to a particular telephone, Title III would violate the Fourth Amendment requirement of particularity. TIA Comments at 36 n. 86. But TIA goes on to rebut its own argument, conceding that this proposition would be true only to the extent that the intercepted call "does not involve any facilities identifiable with the subscriber." Ibid. Of course, any possible interpretation of "facilities" under Title III must link the communications
(continued...)

As a matter of historical fact, it is generally true that the telecommunications facilities for which interception authority was granted were associated with fixed, physical equipment, usually the subscriber's local loop.¹⁴ See also CDT Comments at 39 (arguing that "facilities" "has a physical connotation"). Congress enacted CALEA, however, precisely because advances in telecommunications technology had greatly reduced the value of interceptions made at the level of the local loop, and Congress wanted to "preserve the government's ability, pursuant to court order, to intercept communications that utilize advanced technologies." House Report at 16. The FBI Director had explained to Congress that new multiplexing capabilities, coupled with advanced communications services and features, "undermine the necessity for communications to be transmitted always to the same specific location or through the same wireline loop." *Ibid.*¹⁵ Indeed, the deployment of sophisticated digital technology generally disassociates a telephone subscriber's

¹³(...continued)

facilities to the subscriber, and it makes no sense to suggest that only a definition that equates "facilities" with "particular telephone" could demonstrate the requisite degree of connection.

Moreover, TIA's reliance upon United States v. Tavaréz, 43 F.3d 1136 (10th Cir. 1994) is misplaced. See TIA Comments at 35 n. 80. The court in Tavaréz explicitly based its holding upon the language of the state statute that formed the basis for the interception at issue. See 43 F.3d at 1139 ("usage of the term ["facilities"] in other provisions of the Oklahoma Act indicates that "facilities" means target telephones * * * "facilities" is used elsewhere in the Oklahoma Act to mean the targeted telephones").

¹⁴ "[T]raditionally, common carriers have offered essentially 'fixed point' telecommunications * * * transmitted over common carrier facilities, such as telephone wires that were dedicated to a customer's specific telephone number (often referred to as a subscriber's 'loop')." Joint Hearings at 24 (prepared statement of Louis J. Freeh).

¹⁵ See also Joint Hearings at 43 (Responses of Louis J. Freeh to Questions Submitted by Senator Leahy) ("As the features and services being deployed and offered by service providers have become more advanced, the communications and dialing information that law enforcement agencies attempt to intercept and acquire become less accessible in the local loop, *and* effective central office access has not been developed by the telephone companies").

communications facilities from particular pieces of physical equipment, because functions that were formerly performed by dedicated hardware are now performed by software that employs whatever hardware may be available at least cost to the system. See John Bellamy, Digital Telephony at 441 (2d ed. 1991) (describing virtual circuit networks and explaining that "a virtual circuit is a logical concept involving addresses and pointers in the nodes of the network, but no dedicated transmission facilities").

Congress understood these concerns when it enacted CALEA. Congress did not specify in CALEA that the telecommunications industry must preserve law enforcement's interception capabilities by routing all calls through the local loop. Rather, Congress encouraged industry to implement new technologies, but required carriers to develop and deploy the capability for allowing law enforcement to intercept, "pursuant to a court order or other lawful authorization, * * * all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities or services of a subscriber of such services." CALEA, § 103(a)(1). Thus, Congress did not allow technological changes to have the effect of limiting law enforcement's existing interception authority under Title III; rather, it took steps to ensure that advanced telecommunications systems would retain the capability to deliver meaningful interceptions within the well-established scope of that authority. See House Report at 10 (stating that "[t]he purpose of [CALEA] is to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications using advanced technologies such as digital or wireless transmission modes, speed dialing and conference calling"). Contrary to the commenters' assertions, therefore, the capabilities mandated by CALEA include the ability to intercept conference calls in their entirety, even if the

subscriber puts other parties to the call on hold or leaves the call altogether, and Title III permits law enforcement to intercept every leg of a call carried "to or from the equipment, facilities or services" of the subscriber, regardless of whether the subscriber is on the line.

B. The Scope of "Call-Identifying Information"

1. We now turn from Section 103(a)(1) of CALEA, which concerns the interception of communications, to Section 103(a)(2), which concerns access to "call-identifying information." A number of the capabilities missing from the interim standard involve the failure to ensure law enforcement's access to call-identifying information. CALEA specifically defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2). The government's petition explains why each of the capabilities in question involves "call-identifying information" within the scope of this statutory definition.

Beginning at a relatively early stage in the standard-setting process, industry adopted its own, highly restrictive, definition of "call-identifying information," a definition that is now part of the interim standard. See J-STD-025 § 3. The industry definition forms the basis for many of the arguments by TIA and other commenters regarding the assistance capabilities in the government's petition. However, industry's definition is deeply flawed and fundamentally inconsistent with CALEA's underlying goal of "preserv[ing] the government's ability" to carry out legally authorized electronic surveillance. House Report at 9, reprinted in 1994 USCCAN at 3489. Therefore, before

we address particular assistance capabilities involving call-identifying information, we first discuss why industry's definition of "call-identifying information" is incorrect.¹⁶

To understand the scope of "call-identifying information," the legislative history surrounding the term must be reviewed. The original draft of the bill that evolved into CALEA did not use the term "call-identifying information" at all. Instead, it referred to "call setup information." See Joint Hearings at 267-68. "Call setup information" was defined in the draft bill as "the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization, including information associated with any telecommunication system dialing or calling features or services." Ibid.

During the course of the legislative process, Congress replaced "call setup information" with "call-identifying information." In doing so, Congress not only changed the operative term, but also clarified and expanded the scope of the statutory definition. As defined in CALEA, "call-identifying information" explicitly covers both dialing information and signaling information. 47 U.S.C. § 1001(2).¹⁷ Moreover, while "call setup information" was confined to information identifying the

¹⁶ Law enforcement specifically objected to the language of industry's definition during the standard-setting process (see DOJ/FBI Petition, Appendix 3, p. 2), and the government has omitted industry's definition from the proposed rule that accompanies the government's rulemaking petition. To the extent that TIA seems to suggest that the government has not taken issue with the industry definition (see TIA Comments at 38), it therefore is simply wrong.

¹⁷ CDT attempts to read "signaling information" out of the statutory definition. See CDT Comments at 22-24. CDT asserts that signaling information "includes nothing beyond 'dialing' information" and that signaling is "coextensive" with "dialing." Id. at 22-23. This reading of the statutory definition renders "signaling information" redundant. It therefore conflicts with the elementary principle that "legislative enactments should not be construed to render their provisions mere surplusage." Dunn v. CTFC, 117 S. Ct. 913, 917 (1997); Bennett v. Spear, 117 S. Ct. 1154, (continued...)

"origin" and "destination" of communications, "call-identifying information" includes not only "origin" and "destination," but the "direction" and "termination" of communications as well. Ibid.¹⁸

The definition of "call-identifying information" employed in the interim standard effectively disregards the changes that Congress made when it replaced "call setup information" with "call-identifying information." In particular, the industry definition deprives "direction" and "termination" of their intended scope. The interim standard defines "direction" as "the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party)." Information identifying redirected-to and redirected-from parties, however, was already encompassed within "origin" and "destination." Moreover, by focusing exclusively on redirected-to and redirected-from parties, the interim standard effectively turns "direction" into "redirection." Similarly, the interim standard defines "termination" as "the number of the party ultimately receiving a call (e.g., answering party)," yet "destination" was sufficient to capture that information. If Congress had intended to cover only the information identified in the interim standard, it would not have had to add "direction" and "termination" to the statutory definition at all. The interim standard thus comes perilously close to reading "direction" and "termination" out of the statute.

¹⁷(...continued)

1167 (1997) ("[i]t is our duty to give effect, if possible, to every clause and word of a statute") (internal quotation marks omitted).

¹⁸ CDT asserts that Congress intended for "call-identifying information" to have the same meaning as "call setup information." See CDT Comments at 25-26. If that had been Congress's intent, Congress would not have had to change the term in the first place, much less revise the statutory definition of the term.

The industry definition also results in the exclusion of a wide range of dialing and signaling information to which law enforcement traditionally has had access in the POTS environment. As explained in the petition, law enforcement traditionally has been able to capture all of the dialing and signaling information used for call processing that traverses the "local loop" between the subscriber and the central office. Thus, for example, law enforcement could detect tones and signaling information indicating call waiting, a conference call, or the transfer of a call. DOJ/FBI Petition ¶ 58. Similarly, law enforcement could detect signaling information indicating how the network treated a call attempt, such as ringing or a busy tone. *Id.* ¶ 81. These kinds of information have substantial investigatory and evidentiary value for law enforcement. Nevertheless, the industry definition purports to exclude this kind of dialing and signaling information from the scope of Section 103 altogether.

As noted above, we do not contend that law enforcement's traditional electronic surveillance capabilities are dispositive regarding the reach of CALEA. See pp. 10-11 *supra*. But at the very least, the Commission should not assume that Congress intended to narrow the scope of law enforcement's capabilities in this fashion without compelling evidence of such a purpose. No such evidence has been presented.

Several commenters point to a passage in the House Report that states that, "[f]or voice communications, [call-identifying] information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier's network." House Report at 21, reprinted in 1994 USCCAN 3501 (emphasis added). As the use of the word "typically" indicates, however, this

passage is meant to provide only an illustration, not a definition, of "call-identifying information."¹⁹

In the balance of the passage, the House Report states that "[o]ther dialing tones * * * that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information." Ibid. (emphasis added). If the language relied on by the commenters had been intended as an exhaustive definition of "call-identifying information," as the commenters suggest, Congress would have had no reason to include the underscored language; rather, it would have said without qualification that no other dialing or signaling tones constitute call-identifying information.

The government's rulemaking petition rests on a less crabbed reading of the statutory language than the one employed in the interim standard. In particular, the government's petition employs a more natural and logical reading of "direction" and "termination."²⁰

Read naturally, "information identifying * * * the direction" of a communication encompasses not only information about the path of the communication through a network, but also information about any dialing and signaling activity by the subscriber that directs the communication. For example, when the subscriber presses a flash hook or feature key to transfer

¹⁹ The illustrative, non-comprehensive nature of the passage is further indicated by the fact that it refers only to the "origin" and "destination" of communications, while the statutory definition of call-identifying information also includes "direction" and "termination." Compare House Report at 21, reprinted in 1994 USCCAN at 3501 (call-identifying information "identifies the origin and destination of a wire or electronic communication"), with 47 U.S.C. § 1001(2) (call-identifying information means information "that identifies the origin, direction, destination, or termination of each communication * * * ").

²⁰ Although our discussion here focuses principally on "direction" and "termination," the interim standard's definitions of "origin" and "destination" are likewise unduly restrictive. The interim standard defines "origin" as "the number of the party initiating a call" and "destination" as "the number of the party to which a call is being made (e.g. called party)." These definitions exclude obvious call-identifying information, such as temporary local directory numbers for mobile call routing and routing numbers for ported calls.

or forward the call, he is engaged in directing the call. Carriers therefore are obligated under Section 103(a)(2) to provide a message that identifies such instances of call direction.

As for "termination," a call attempt may "terminate" in a variety of ways: with an answer by the called party, with ringing (without an answer), with a busy tone or a trunk busy signal, with automatic redirection to a voice mail box, or in other ways. "Information identifying * * * the termination" of a communication therefore encompasses not only the number of the answering party, but also information perceived by the subject about how the call terminated -- information reflected, for example, by busy tones or "stutter" dial tones. All such signaling information comes within the statutory definition of "call-identifying information."

When "call-identifying information" is read in this common-sense manner, law enforcement's traditional capabilities regarding the acquisition of dialing and signaling information are preserved rather than impaired. And when the corresponding shortcomings in industry's restrictive definition of "call-identifying information" are kept in mind, a large share of the commenters' objections to the government's petition fall away.

2. CALEA requires a carrier to provide access to all call-identifying information that is "reasonably available to the carrier * * * ." 47 U.S.C. 1002(a)(2). A number of commenters assert that, for one reason or another, particular dialing and signaling information sought in the government's petition is not "reasonably available" and that the interim standard is therefore not deficient in failing to require delivery of such information. See, e.g., Nextel Comments at 11; USTA Comments at 5; PrimeCo Comments at 14; CDT Comments at 43.

To the extent that these comments are directed at particular types of call-identifying information, we address them individually in the relevant sections of the discussion below.

However, three points regarding the general issue of "reasonable availability" should be made at the outset.

First, we strongly disagree with those commenters who suggest that the potential cost of delivering particular call-identifying information to law enforcement is, by itself, a basis for deeming the information "not reasonably available." Congress understood that compliance with Section 103's assistance capability requirements might be prohibitively expensive in particular cases. But there is no indication that Congress meant for the "reasonably available" language of Section 103(a)(2) to deal with that problem. Instead, Congress provided for relief under Section 109(b) of CALEA, which excuses carriers from meeting assistance capability requirements that are not "reasonably achievable" with respect to particular equipment, facilities, and services unless the government pays the additional reasonable costs of compliance. See 47 U.S.C. § 1008(b). The statutory standards for "reasonable achievability" under Section 109(b) expressly incorporate cost concerns. See *id.* § 1008(b)(1)(B), (D), (E), (H). In contrast, there is nothing in the language or legislative history of Section 103(a)(2) that suggests that Congress intended for cost considerations to govern the underlying scope of carriers' assistance capability obligations. Issues of "reasonable availability" under Section 103(a)(2) should focus on technical issues rather than the kinds of financial issues that are addressed in Section 109(b) and elsewhere in CALEA.²¹

²¹ Several commenters note that the government recently has received CALEA cost estimates from manufacturers and shortly will present Congress with an implementation report that discusses cost issues. See AirTouch Comments at 5; US West Comments at 22, 26. The proprietary information provided by manufacturers is subject to non-disclosure agreements (NDAs) that severely limit the ability of the government to disclose cost data. To the extent that the implementation report discusses cost issues, it does so in aggregate terms that do not discuss the costs associated with individual "punch list" items. Even the aggregated cost information in the implementation report is subject to NDA limitations and is being provided to Congress only with the express permission
(continued...)

Second, the commenters are wrong when they suggest that call-identifying information should not be regarded as "reasonably available" unless there is a "business purpose" for making such information available." TIA Comments at 39 (emphasis added); Nextel Comments at 11. "Business purpose" can hardly be the touchstone for analysis under Section 103. Congress imposed the assistance capability requirements of Section 103 precisely because carriers following the dictates of "business purposes" cannot be expected to provide law enforcement with the kind of assistance that is needed to perform authorized electronic surveillance. By virtue of CALEA, "telecommunications carriers * * * are [now] required to design and build their switching and transmission systems to comply with the legislated requirements." House Report at 18, reprinted in 1994 USCCAN at 3498 (emphasis added). Whether providing particular information serves a "business purpose" of the carrier is simply irrelevant to whether the carrier must incorporate the delivery of such information to law enforcement in the design of its network.

Third, questions of "reasonable availability" do not necessarily lend themselves to generic, across-the-board answers. Delivering particular call-identifying information to law enforcement may be technically straightforward with respect to one platform or network architecture and considerably more difficult and complex with respect to another. Thus, particular call-identifying information may prove to be "reasonably available" to one carrier and not "reasonably available" to another.

The Commission does not have to establish that particular call-identifying information is "reasonably available" to all carriers in all circumstances in order for such information to be included

²¹(...continued)

of the manufacturers involved. If the manufacturers are willing to grant written permission with respect to the Commission, the government would accede to their request and provide a copy of the report to the Commission.

in standards issued under Section 107(b). As explained above, standards issued by the Commission are simply a safe harbor; no carrier is legally obligated to use the means set forth by the Commission if it believes that it can satisfy its underlying assistance capability obligations under Section 103 in another manner. See pp. 13-14 supra. As a result, the Commission does not have to dilute its standards to account for the possibility that call-identifying information that is "reasonably available" for some carriers may not be "reasonably available" for all.

At the same time, an assertion that particular call-identifying information is not "reasonably available" with respect to particular platforms is not sufficient, even if true, to show that the interim standard is not "deficient." As explained above, by virtue of CALEA's safe-harbor provision, the interim standard effectively displaces the underlying assistance capability requirements of Section 103 for carriers that implement the interim standard. See pp. 12-13 supra. If particular call-identifying information is "reasonably available" to some of the carriers covered by the interim standard, the failure of the interim standard to include such information renders the interim standard deficient, regardless of whether the same information is equally available to other carriers.

C. Post-Cut-Through Dialing

1. The first capability concerning call-identifying information that is missing from the interim standard is the delivery of "post-cut-through" dialed digits. As explained in the government's petition, post-cut-through dialing is used in long distance calls, credit card calls, and (in some instances) local calls to complete the call and reach the intended party. DOJ/FBI Petition ¶ 66. For reasons set forth in the petition, post-cut-through dialing used to complete calls has important investigatory and evidentiary value to law enforcement. Id. ¶¶ 68-71. Post-cut-through dialing and signaling information that completes a call is "dialing or signaling information" that identifies the

"destination" of the call, placing it directly within CALEA's definition of "call-identifying information" (47 U.S.C. § 1001(2)). *Id.* ¶ 69. As a result, the interim standard's failure to require delivery of post-cut-through dialing used to complete calls renders the standard deficient.

In response to the government's petition, many of the commenters point out that a subscriber may engage in post-cut-through dialing for purposes other than call completion. In particular, a subscriber may dial digits after the cut-through in order to control or otherwise interact with equipment of the called party. For example, a subscriber might enter a PIN number to access his bank account information, or he might make numeric selections from a voice-mail menu to access other kinds of information.

We readily acknowledge that, in some instances, post-cut-through digits are dialed for purposes other than call completion and do not represent the number of a called party. In those instances, we do not contend that the post-cut-through digits constitute "call-identifying information." But when post-cut-through digits are dialed for call completion, they "identif[y] the * * * destination * * * of [a] communication" and therefore come squarely with the statutory definition of "call-identifying information."

The legislative history of CALEA reflects this distinction. As noted above, the House Report's discussion of call-identifying information states that "[o]ther dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information." House Report at 21, reprinted in 1994 USCCAN at 3501 (emphasis added). As the underscored language shows, Congress did not exclude post-cut-through dialing from the scope of "call-identifying information" altogether; it simply indicated that post-cut-through dialing is excluded when it is "used to signal customer premises equipment of the

recipient." The testimony of the FBI Director reflects the same distinction. See, e.g., Joint Hearings at 50 ("What I want with respect to pen registers is the dialing information"; "[a]s to the banking accounts and what movies someone is ordering at Blockbuster, I do not want it [and] do not need it" under pen register authority). Contrary to the suggestion of some of the commenters (e.g., CDT Comments at 42-43; AT&T Comments at 8-9), nothing in the legislative history even remotely suggests that Congress intended to treat post-cut-through dialing used for call completion as anything other than "call-identifying information."

Several commenters argue that because post-cut-through dialing is not always call-identifying information, carriers are not obligated to provide access to post-cut-through dialing at all. See, e.g., TIA Comments at 45-46; CDT Comments at 43. They base this argument on Section 103(a)(4)(A) of CALEA, which directs carriers to assist law enforcement surveillance activities "in a manner that protects * * * the privacy and security of communications and call-identifying information not authorized to be intercepted * * * ." 47 U.S.C. § 1002(a)(4)(A). They argue that Section 103(a)(4)(A) prohibits carriers from giving law enforcement post-cut-through digits that are not involved in call completion. Because carriers currently lack any technological means to discriminate between post-cut-through digits dialed for call completion and digits dialed for transactional purposes, the commenters reason that the only way for carriers to comply with Section 103(a)(4)(A) is not to provide post-cut-through digits at all.

The short answer to this argument is that Section 103(a)(4)(A) has nothing to do with the issue of post-cut-through dialing. Congress understood that pen register surveillance could result in the delivery of transactional dialing information, but it dealt with that problem through Section 207 of CALEA, not Section 103(a)(4)(A). See House Report at 31-32, reprinted in 1994 USCCAN

at 3511-12. Section 207, now codified as 18 U.S.C. § 3121(c), provides that a law enforcement agency using pen registers "shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." Section 207 presupposes that carriers will deliver transactional data to law enforcement in the course of carrying out pen register orders. Rather than prohibit carriers from doing so, Congress instead chose to impose a technology-based minimization obligation on law enforcement.²²

Some commenters argue that the interim standard is not deficient because law enforcement can obtain post-cut-through dialed digits as part of call content by serving the subscriber's local carrier with a Title III order. See TIA Comments at 42-43; PrimeCo Comments at 13. But when a subscriber dials post-cut-through digits to complete a call, the dialed digits are call-identifying information, not call content, and law enforcement is entitled to acquire them with a pen register order. Forcing law enforcement to meet the heightened requirements of Title III in order to acquire post-cut-through digits is therefore inconsistent both with CALEA and with the structure of the underlying electronic surveillance statutes.²³

Alternatively, some commenters suggest that law enforcement can obtain post-cut-through digits by serving a pen register order or a subpoena on the carrier that provides the long distance

²² Even taken on its own terms, without regard to Section 207, the commenters' reliance on Section 103(a)(4)(A) is misplaced. Section 103(a)(4)(A) does not purport to override a carrier's unqualified obligation under Section 103(a)(2) to provide access to reasonably available call-identifying information. A carrier therefore cannot invoke Section 103(a)(4)(A) as a "defense" to its failure to meet its obligations under Section 103(a)(2).

²³ TIA asserts that post-cut-through dialed digits are not call-identifying information "for the initial carrier." TIA Comments at 44. But neither the statutory definition of "call-identifying information" nor the statutory obligation to provide access to call-identifying information is tied to whether "the initial carrier," as opposed to another carrier, uses the digits to complete the call. See 47 U.S.C. §§ 1001(2), 1002(a)(2).

service. See TIA Comments at 42; CDT Comments at 42. This argument is both legally and practically misconceived. As a legal matter, nothing in Section 103(a)(2) relieves a carrier of its obligation to "expeditiously isolat[e] and enabl[e] the government * * * to access call-identifying information" when the information is (or is claimed to be) available from another source. As a practical matter, the "solution" of turning to the long-distance carrier is no solution at all. Thousands of carriers provide long-distance calling card and credit card services; a subject can choose from among all of them and may change from one to another with each successive call. Law enforcement cannot possibly determine which particular long-distance provider is being used by the subject for a particular call and acquire the dialed digits sent to the provider in anything like real time. Congress understood that law enforcement needs to acquire call-identifying information contemporaneously with the calls to which it relates; it is for that reason that Section 103(a)(2) obligates carriers to provide call-identifying information "expeditiously" and "before, during, or immediately after" the transmission of the associated communication. Serving a long-distance carrier with a subpoena to get post-cut-through digits from billing records is patently inadequate to meet the law enforcement needs that Congress acknowledged and incorporated into Section 103(a)(2).²⁴

Finally, a number of commenters assert that post-cut-through dialed digits are not "reasonably available" to local carriers because detecting them would require potentially expensive modifications

²⁴ The problem is particularly acute when prepaid calling cards are used. A long-distance provider has no need to keep track of who is using a prepaid calling card; it merely debits the account associated with the card as long-distance calls are made. When a subject uses a prepaid card, law enforcement therefore could not obtain the desired dialing information from the provider at all unless law enforcement somehow knew the account number of the card that the subject was using. In some cases, moreover, long-distance providers do not even maintain records of the number being called. Since the rate per minute for calls made with prepaid calling cards is usually fixed and does not depend on the distance between the calling and called parties, a long distance carrier may have no need to maintain a record of the called number for billing purposes.

of existing equipment. See TIA Comments at 44-45; USTA Comments at 7; Ameritech Comments at 6-7; BellSouth Comments at 15; PrimeCo Comments at 13. To capture post-cut-through digits for delivery to law enforcement, a carrier may apply a tone decoder to the call or detect the dialed digits outside the switch by a "loop-around" or other means.²⁵ The commenters note that tone decoders are shared resources, which ordinarily are freed for use on other calls after a particular call has been cut through; in order to detect dialed digits after cut-through, a tone decoder will have to be dedicated to the call content channel for the duration of the call. The commenters add that some technologies (such as cellular and PCS) may not currently be configured to detect touch tones at all and therefore will have to add this capability. See BellSouth Comments at 15; USTA Comments at 7.²⁶

It is certainly true that carrier equipment will have to be modified in order to detect and extract post-cut-through digits. However, neither that fact nor the potential expense of the modifications means that the information is not "reasonably available." Congress understood that telecommunications carriers would be "required to design and build their switching and transmission

²⁵ We note that the current Signaling System 7 (SS7) protocol already has an option to have the number of the answering party returned as part of the SS7 Answer message. This option has not been deployed in the United States, but it has been deployed in several other parts of the world. If it were deployed here, the local carrier would be able to determine post-cut-through digits used for call completion without any need to monitor the post-cut-through data stream itself.

²⁶ TIA states that delivery of post-cut-through digits would be especially difficult when a subscriber uses a "voice recognition dialing" feature (a feature that allows the subscriber to designate a called party by saying the party's name or other identifying word rather than by dialing the number). TIA Comments at 45. The government's petition does not seek the delivery of the translated digits generated by voice recognition dialing unless the carrier (or a provider of telecommunications support services under the carrier's control) is the one performing the translation. Thus, in the typical post-cut-through case where the voice recognition dialing feature is implemented by a long-distance carrier, the local carrier would be under no obligation to provide access to the translated digits (or the actual words spoken to use the feature).

systems to comply with the legislated requirements" of CALEA. House Report at 18, reprinted in 1994 USCCAN at 3498. As explained above, the costs associated with system modifications are appropriately dealt with through the reimbursement provisions of Section 109(b), not the assistance capability requirements of Section 103. See p. 36 supra. If "the total cost of compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features" (House Report at 28, reprinted in 1994 USCCAN at 3508), relief is available under Section 109(b). Otherwise, the cost of implementation should not excuse carriers from providing what is unquestionably call-identifying information.

2. The government's proposed rule provides for post-cut-through dialed digits to be delivered to law enforcement on a call data channel rather than a call content channel. DOJ/FBI Petition, Appendix 1 (§ 64.1708(i)(1)). The proposed rule contains a similar provision regarding the delivery of notification messages for network-generated in-band and out-of-band signaling (see pp. 55-59 infra). Id. § 64.108(d).

TIA argues that the failure to provide this information on a call data channel does not render the interim standard "deficient" and that the Commission therefore cannot include such a requirement in its standards. TIA Comments at 61-62. As noted in the government's rulemaking petition, we agree that a carrier can satisfy its assistance capability obligations under Section 103 without necessarily delivering such information on a call data channel. See DOJ/FBI Petition ¶ 84. However, it does not follow that the Commission is powerless to address this issue as part of the present proceeding.

As explained above, the interim standard does not require the delivery of post-cut-through dialed digits at all. That omission renders the interim standard deficient and thereby triggers the

Commission's authority under Section 107(b). Once the Commission is authorized to act under Section 107(b), it may take a variety of considerations into account in framing an appropriate standard. See 47 U.S.C. § 1006(b)(1)-(5). Among other things, the Commission may consider the cost-effectiveness and privacy impact of alternative solutions. Id. § 1006(b)(1), 1006(b)(2).

As explained in the government's petition, requiring the government to use both a call data channel and a call content channel when it is engaged in pen register surveillance results in needless duplication of equipment, facilities, and cost. DOJ/FBI Petition ¶ 84. In addition, delivery of post-cut-through digits to law enforcement over a call content channel creates an unnecessary risk of inadvertent intrusions on call content when the government is seeking (and is specifically authorized to seek) only call-identifying information. Id. ¶ 85. For these reasons, if the Commission agrees that Section 103(a)(2) obligates carriers to provide law enforcement with post-cut-through digits, the Commission appropriately may include the use of a call data channel for the delivery of such information in the Commission's standards.²⁷

D. Other Subject-Initiated Dialing and Signaling

In addition to omitting post-cut-through dialed digits, the interim standard also fails to require carriers to provide law enforcement with other important kinds of subject-initiated dialing and signaling information. As explained in the government's petition, an intercept subject (either the subscriber or another person using the subscriber's telephone) may invoke services like three-way calling and call transfer by pressing feature keys or the flash hook. DOJ/FBI Petition ¶ 61. The interim standard fails to provide a call data message when the intercept subject inputs dialing or

²⁷ TIA suggests that delivery of post-cut-through digits over the call data channel is a new request that was not part of law enforcement's "punch list." That is incorrect. See, e.g., DOJ/FBI Petition, Appendix 2, p. 33; id. Appendix 3, p. 16.

signaling information within a call in this fashion. For reasons set out in the government's petition, this kind of information constitutes "call-identifying information" under CALEA, and without access to it, law enforcement may find it difficult or impossible to follow the course of the communication or to determine to whom the subject is speaking at any point in the conversation. Id. ¶¶ 62-65.

A number of commenters assert that information identifying subject-initiated dialing and signaling activity is not "call-identifying information," and therefore need not be provided, because it does not identify the "origin, direction, destination, or termination" of a communication (47 U.S.C. § 1001(2)). See, e.g., TIA Comments at 47; CDT Comments at 44-45; BellSouth Comments at 10. These arguments all rest in one fashion or another on the industry definition of "call-identifying information" contained in the interim standard. That definition, however, is improperly restrictive and is not faithful to the law enforcement objectives of CALEA. See pp. 30-35 supra. Application of that definition to the subject-initiated dialing and signaling activity identified in the government's petition would result in a dramatic and wholly unwarranted loss of information with important investigatory and evidentiary value.

Properly interpreted, the statutory definition of "call-identifying information" is amply sufficient to include subject-initiated dialing and signaling activity like the pressing of flash hooks and feature keys to control call forwarding and call transfer. This activity identifies the "direction" and "destination" of the subject's communications. As explained above (see pp. 34-35 supra), "information identifying * * * the direction" of a communication encompasses not only information about the path of the communication through a network, but also information about dialing and signaling activity by the subscriber that directs the communication. When the subject presses a flash hook or feature key to transfer a call or establish a conference call, he is engaged in directing the call,

and the carrier is obligated to provide information identifying that "direction." By the same token, information about flash hook and feature key activity is necessary to identify the "destination" of each communication, for without such information, it may be impossible to tell with which party the subject is communicating. As explained in the government's petition, all of this information traditionally has been accessible to law enforcement over the local loop.

CDT asserts that information identifying the persons participating in a call is outside the scope of the pen register statute and that the government therefore is demanding information to which it is not legally entitled. CDT Comments at 44-45. This argument is misconceived in two respects. First, while pen registers and trap-and-trace devices do not directly report the identities of calling and called parties, they provide calling information that law enforcement legitimately may use, in conjunction with other information, to identify persons involved in criminal activity. There is nothing remotely improper, much less unlawful, about such investigatory uses of pen register information. Therefore, the suggestion that acquiring information about subject-initiated dialing and signaling activity is somehow inimical with the purposes of the pen register statute is baseless.

Second, CDT's argument assumes that information about subject-initiated dialing and signaling activity (and "call-identifying information" more generally) is only relevant and only sought in pen register cases. That is obviously incorrect. Information about subject-initiated dialing and signaling activity is just as important to law enforcement under Title III as it is in pen register cases, if not more so, and a carrier's statutory obligations under Section 103 apply to Title III cases

as well as to pen registers. Yet CDT's argument would deprive law enforcement of the capability to acquire this information in all cases, even those involving wiretaps under Title III.²⁸

Taking a different tack, TIA asserts that, for signaling activity that is transmitted from the subject to the network and detected by the switch, the interim standard already provides law enforcement with "all potentially relevant call-identifying information." TIA Comments at 48-49 (emphasis in original). TIA bases this argument on the interim standard's Change message (J-STD-025 § 5.4.4) and certain other messages. Contrary to TIA's claim, however, these messages are not an adequate substitute, practically or legally, for the information sought in the government's petition.

The principal shortcoming involves the operation of the Change message. The Change message is generated by changes in call identities. See J-STD-025 § 5.4.4 (Change message triggered when, e.g., "two or more call identities are merged into one call identity" or when "an additional call identity is associated with an existing call"). However, changes in call identities need not -- and for some platforms will not -- correspond to changes in party identities. Manufacturers are free to use a single call identity to cover multiple legs of a call. When this approach is used, subject-initiated signaling activity will not generate a Change message. For example, a subject could

²⁸ As a general matter, none of the assistance capability issues in this proceeding requires the Commission to determine which provision of the federal electronic surveillance statutes authorizes law enforcement to obtain particular information. Section 103(a) of CALEA requires carriers to maintain the capability to provide access to communications and call-identifying information "pursuant to a court order or other lawful authorization." 47 U.S.C. § 1002(a)(1), 1002(a)(2). As long as law enforcement could obtain a "court order or other lawful authorization" to acquire the information in question, it is irrelevant for present purposes whether the information could be acquired pursuant to a pen register order (see 18 U.S.C. § 3123) or whether the government instead would need a Title III intercept order (see id. § 2518) or some other form of legal authorization.